PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
H04B 7/216, H04L 9/00, H04Q 7/22

A1

(11) International Publication Number: WO 00/24139

(43) International Publication Date: 27 April 2000 (27.04.00)

(21) International Application Number: PCT/US99/24521

(22) International Filing Date: 19 October 1999 (19.10.99)

(30) Priority Data:
09/176,650 21 October 1998 (21.10.98) US

(71) Applicant: QUALCOMM INCORPORATED [US/US]; 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

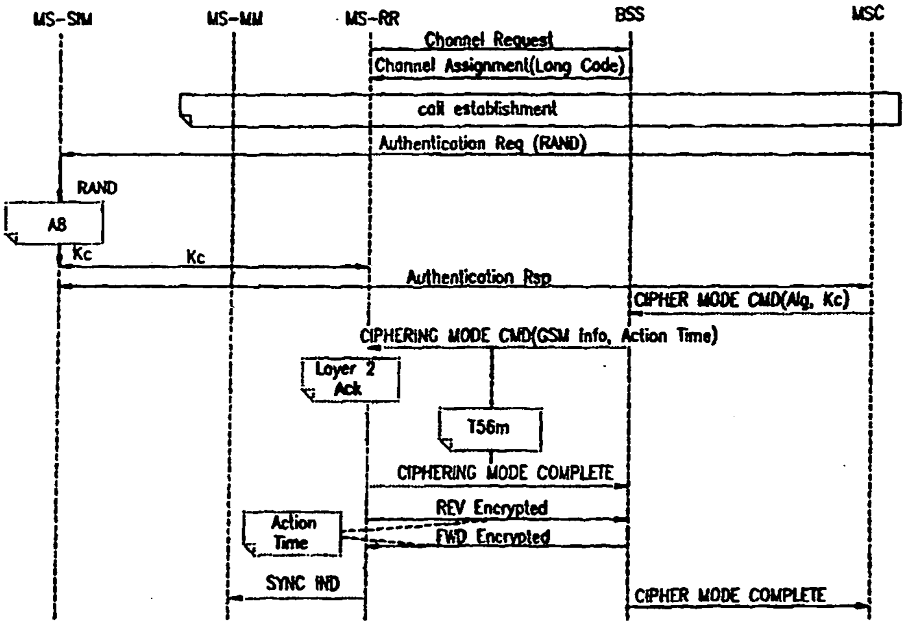
(72) Inventors: NEVO, Ron; Mitzpe Aviv, 20187 Misgav (IL). VAKULENKO, Michael; Harav Ankave 22/19, 35849 Haifa (IL). QUICK, Franklin, Jr.; 4502 Del Monte Avenue, San Diego, CA 92107 (US). KOLOR, Sergio; Nahshon 4/1, 34612 Haifa (IL). NIZRI, Shlomo; David Hamelekh 18, 14279 Tiberias (IL). LEVY, Atai; Oren Street 7, 34612 Haifa (IL).

(74) Agents: OGROD, Gregory. D. et al.; Qualcomm Incorporated, 5775 Morehouse Drive, San Diego, CA 92121-1714 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: ENCRYPTION SUPPORT IN A HYBRID GSM/CDMA NETWORK



(57) Abstract

In a GSM mobile wireless telecommunications system, a method for encrypting data for transmission over a CDMA air interface includes providing a GSM encryption key and transmitting an indication of the key over the CDMA air interface. The data are encrypted for transmission over the CDMA air interface using the key.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav	TM	Turkmenistan
BF	Burkina Faso	GR	Greece		Republic of Macedonia	TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's	NZ	New Zealand		
CM	Cameroon		Republic of Korea	PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

ENCRYPTION SUPPORT IN A HYBRID GSM/CDMA NETWORK

FIELD OF THE INVENTION

The present invention relates generally to wireless telecommunications, and specifically to advanced cellular telephone networks.

BACKGROUND OF THE INVENTION

The Global System for Mobile (GSM) telecommunications is used in cellular telephone networks in many countries around the world. Existing GSM networks are based on time-division multiple access (TDMA) digital communications technology. GSM offers a useful range of network services and standards, including encryption of user data and signaling to protect confidentiality of communications. GSM encryption is powerful, i.e., relatively secure against cryptanalytic attack, but generally requires special-purpose hardware to cipher and decipher the data and signaling. GSM network security features, including ciphering, are defined by GSM standards 02.09 and 03.20, which are incorporated herein by reference. The encryption itself uses proprietary algorithms defined by the GSM MoU Group of participant companies, such as the A5 algorithms for ciphering and the A8 algorithm for generation of an encryption key K_c used in ciphering, as defined by GSM standards.

Code-division multiple access (CDMA) is an improved digital communications technology, which affords more efficient use of radio bandwidth than TDMA, as well as a more reliable, fade-free link between cellular telephone subscriber units (or mobile stations) and base stations. The leading CDMA standard is IS-95, promulgated by the Telecommunications Industry Association (TIA) and incorporated herein by reference. IS-95 specifies a public long code mask, based on an electronic serial number (ESN), which is used to spread the spectrum of user data and signaling before transmission over traffic channels. The ESN itself is transmitted by the subscriber unit over an access channel, making it relatively difficult for an eavesdropper to capture the code and thereby decrypt the call. Spreading using the long code provides only limited protection against cryptanalysis, however. IS-95 also describes a method of spreading using a private long code, based on secret data, so as to afford greater protection against eavesdropping.

PCT patent application PCT/US96/20764 which is based upon U.S. patent application serial no. 08/575,413 entitled "Wireless Telecommunications System Utilizing CDMA Radio Frequency Signal Modulation in Conjunction with the GSM A-Interface Telecommunications Network Protocol," filed December 20, 1995, which are assigned to the assignee of the present patent application and both incorporated herein by reference, describe a wireless telecommunications system that uses a CDMA air interface (i.e., basic RF communications protocols) to implement GSM network services and protocols. Using this system, at least some of the TDMA base stations (BSSs) and subscriber units of an existing GSM network would be replaced or supplemented by corresponding CDMA equipment. CDMA BSSs in this system are adapted to communicate with GSM mobile switching centers (MSCs) via a standard GSM A-interface. The core of GSM network services is thus maintained, and the changeover from TDMA to CDMA is transparent to users.

Hybrid cellular communications networks, incorporating both GSM and CDMA elements, are also described in PCT patent publications WO 95/24771 and WO 96/21999, and in an article by Tscha, et al., entitled "A Subscriber Signaling Gateway between CDMA Mobile Station and GSM Mobile Switching Center," in Proceedings of the 2nd International Conference on Universal Personal Communications, Ottawa (1993), pp. 181-185, which are incorporated herein by reference. None of these publications deals with specific issues of encryption support.

SUMMARY OF THE INVENTION

It is an object of the present invention to provide methods and apparatus for encryption support in a hybrid GSM/CDMA cellular communications network.

In some aspects of the present invention, methods and apparatus are provided to enable GSM-compatible ciphering and deciphering capabilities over a CDMA air interface.

In preferred embodiments of the present invention, a mixed GSM/CDMA cellular communications system includes one or more CDMA base stations, controlled by a GSM mobile switching center (MSC). Systems of this type are further described in U.S. patent application serial no. 09/119,717 entitled "Base Station Handover in a Hybrid GSM/CDMA Network," filed July 20, 1998, which is assigned to the assignee of the present patent application and is incorporated herein by reference. Communications over a CDMA air interface between a subscriber unit in the system, also referred to herein as a mobile station (MS), and one of the CDMA base stations (BSS) are ciphered and deciphered using a GSM encryption key K_C provided in accordance with GSM standards. The MSC controls ciphering of user data and signaling substantially in accordance with GSM networking protocols. The GSM-based communications system thus supports ciphering over the CDMA air interface with substantially no other modification required to the existing system.

In the context of the present patent application and in the claims, the terms "encryption/decryption" and "ciphering/deciphering" are used interchangeably. While "encryption" and "decryption" are general terms of art, "ciphering" and "deciphering" are more commonly used in GSM standards and systems. There is no substantive difference in the meanings of the corresponding terms.

In some preferred embodiments of the present invention, communications between the MS and the CDMA BSS are ciphered and deciphered using the GSM key K_C in a CDMA-compatible encryption algorithm. Preferably, the algorithm comprises a stream cipher, as is known in the art, which is implemented using a general-purpose microprocessor in the MS, without the need for dedicated encryption hardware.

In other preferred embodiments of the present invention, the communications between the MS and the CDMA BSS are encrypted using a masked pseudorandom noise (PN) long code, in accordance with the IS-95 standard. Masking of the long code provides a shift in the phase, i.e., time shift, of the long code as output by the long code generator so as to produce a unique long code. In the present application the masking of the long code is based upon a private long code mask that is generated based on the GSM K_C. The resulting private long code provides greater security against eavesdropping than can be afforded by open transmission of the usual masked long code. Preferably, the private long code is generated so as to be substantially unique, i.e., so that no two MSs in contact with a given BSS will have the same long code.

In some preferred embodiments of the present invention, the MS is handed over between base stations in the course of a telephone call. Ciphering continues, as described hereinabove, during and after the handover, even when the MS is handed over between a CDMA BSS and a GSM/TDMA BSS.

There is therefore provided, in accordance with a preferred embodiment of the present invention, in a GSM mobile wireless telecommunications system, a method for encrypting data for transmission over a CDMA air interface, including:

providing an encryption key in accordance with GSM ciphering protocols; and

encrypting the data for transmission over the CDMA air interface using the key.

Preferably, providing the encryption key comprises exchanging messages indicative of the key over the CDMA air interface substantially in accordance with GSM ciphering protocols.

Further preferably, encrypting the data includes encrypting user data and signaling.

In a preferred embodiment, encrypting the data includes generating a stream cipher, wherein generating the stream cipher includes generating a cipher using a general-purpose microprocessor.

In another preferred embodiment, encrypting the data includes generating a masked long code based on the encryption key and applying the masked long code to the data. Preferably, generating a long code, generating a long code mask based on the encryption key, and applying the long code masked to the long code and applying the masked long code to the data. The generating of the masked long code includes generating a mask which includes a group of bits based upon a hash function of the key. Preferably, generating the long code mask includes generating a mask which includes a group of bits that is different for calls conducted over the CDMA air interface having the same key.

Preferably, encrypting the data includes continuing to encrypt data substantially without interruption during a handover between two base stations in the system.

Further preferably, encrypting the data includes encrypting using information stored in a subscriber identity module of a mobile station.

There is also provided, in accordance with a preferred embodiment of the present invention, wireless communications apparatus, for use in a GSM mobile telecommunications system, including:

a base station, which receives a GSM encryption key from the system and transmits a message indicative of the key over a CDMA air interface; and

a mobile station, which receives the message and responsive thereto derives the key to be used for encrypting data for transmission over the CDMA air interface.

Preferably, the data encrypted by the mobile station include user data and signaling.

Further preferably, the base station receives the key and transmits the indication in accordance with GSM messaging protocols.

In a preferred embodiment, the mobile station includes a general-purpose microprocessor, which encrypts the data. Preferably, the mobile station includes a subscriber identity module and encrypts the data using information received by the mobile station from the module. Further preferably, the mobile station includes a long code generator, which generates a masked long code mask based upon the key.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be more fully understood from the following detailed description of the preferred embodiments thereof, taken together with the drawings in which:

Fig. 1 is a schematic block diagram of a hybrid GSM/CDMA cellular communications system, in accordance with a preferred embodiment of the present invention;

Figs. 2A and 2B are schematic block diagrams illustrating communications protocols between elements of the system of Fig. 1, in accordance with a preferred embodiment of the present invention;

Fig. 3 is a schematic diagram illustrating message flow associated with encryption in the system of Fig. 1, in accordance with a preferred embodiment of the present invention;

Fig. 4 is a schematic block diagram showing details of a mobile station in the system of Fig. 1, in accordance with a preferred embodiment of the present invention;

Fig. 5 is a schematic block diagram showing details of a base station subsystem in the system of Fig. 1, in accordance with a preferred embodiment of the present invention; and

Fig. 6 is a schematic block diagram illustrating a data structure of a long code mask used in encryption, in accordance with a preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

Reference is now made to Fig. 1, which is a schematic block diagram of a hybrid GSM/CDMA cellular communications system 20, in accordance with a preferred embodiment of the present invention. System 20 is built around a public land mobile network (PLMN) 22, which is based on the GSM communications standard, as is known in the art and described briefly hereinabove. Infrastructure for such networks already exists and is in wide use in many countries, and the present invention has the advantage of enabling gradual introduction of CDMA service is conjunction with such a network without requiring major changes to the existing switching infrastructure.

PLMN 22 comprises at least one mobile-services switching center (MSC) 24, or possibly a number of such centers (although only one MSC is shown here for clarity of illustration), which controls network operations within a geographical area. Among other functions, MSC 24 is responsible for location registration of subscriber units and handover of subscriber units between base stations, as well as linking PLMN 22 to a public switched telephone network (PSTN) and/or packet data network (PDN) 48. The PLMN also comprises a network management center (NMC) 26 and a cell broadcast center (CBC) 28. The functions of these elements, as well as other aspects of system 20 and details regarding a mobile station (MS) 40 in the system, are described further in the above-mentioned U.S. and PCT patent applications.

System 20 includes a plurality of MSs 40, which communicate with PLMN 22 via a plurality of base station subsystems (BSS) 30 and 32 over a wireless RF link at one or more of the accepted cellular communications frequencies. MS 40, which is also known as a subscriber unit, is preferably capable of communicating with both GSM BSS 30, using a standard GSM TDMA radio communications protocol, and CDMA BSS 32, using CDMA-based communication methods described hereinbelow. Although for the sake of clarity, only one each of MS 40, GSM BSS 30 and CDMA BSS 32 is shown in Fig. 1, it will be understood that in actuality, system 20 typically comprises a plurality of each of these system elements.

Both GSM BSS 30 and CDMA BSS 32 communicate with and are controlled by MSC 24, substantially in accordance with GSM standards, i.e., via the GSM standard A-interface, as further described hereinbelow with reference to Figs. 2A and 2B. BSS 32 also communicates with CBC 28, so as to receive messages to be broadcast over the air, and comprises a radio operation and maintenance center (OMC-R) 38, which communicates with

NMC 26 over a GSM-standard Q3 interface. Optionally, BSS 32 may be linked to a general packet data service (GPRS), such as has been proposed by the European Telecommunications Standards Institute (ETSI).

Communications between CDMA BSS 32 and MS 40 are built on a CDMA radio "air interface," which is preferably based on the IS-95 standard for CDMA communications, and most preferably with the TIA/EIA-95-B version of the standard, with necessary modifications as described herein. BSS 32 is built around a base station controller (BSC) 34, which controls and communicates with a number of base station transceivers (BTS) 36. Each BTS transmits RF signals to and receives RF signals from MS 40 when the MS is within a geographical area, or cell, served by the particular BTS. On the other hand, when MS 40 is within a cell served by GSM BSS 30, the MS preferably communicates with BSS 30 over a GSM/TDMA air interface.

MS 40 comprises mobile equipment (ME) 42, which preferably includes either two radio transceivers, one configured for TDMA operation and one for CDMA, or a single transceiver which can dynamically switch between TDMA and CDMA operational modes. MS 40 includes as a part of ME 42 a mobile termination (MT), which supports terminal equipment (TE) 46 for voice and data input and output. In addition, MS 40 comprises a subscriber identity module (SIM) 44, in accordance with GSM standards, which is used in authenticating the identity of a user of MS 40 in a manner substantially transparent to and independent of the CDMA air interface. Although preferred embodiments are described herein with reference to MS 40 having dual CDMA/TDMA air interface compatibility, it will be understood that the principles of the present invention may similarly be applied to systems using mobile stations having only CDMA compatibility or, *mutatis mutandis*, to other systems using GSM networking standards.

Fig. 2A is a block diagram that schematically illustrates protocol stacks used in signaling interfaces between MS 40, CDMA BSS 32 and GSM MSC 24, in accordance with a preferred embodiment of the present invention. These interfaces enable MS 40 to communicate with GSM MSC 24 over a CDMA air interface. Operation of these interfaces, and particularly message flow through these interfaces, is described in greater detail in the above-mentioned PCT application PCT/US96/20764, as well as in the above-mentioned U.S. patent application entitled "Base Station Handover in a Hybrid GSM/CDMA Network." When MS 40 is in communication with MSC 24 via GSM BSS 30, the protocol stacks are in accordance with GSM standards, substantially without modification.

MS 40 communicates with CDMA BSS 32 over a CDMA Um interface, based on a CDMA air interface which is modified for compatibility of signaling with the GSM standard. The CDMA air interface between MS 40 and CDMA BSS 32 comprises CDMA Layer 1, which preferably operates on a standard IS-95 protocol, and GSM-CDMA Layer 2, in which IS-95 operation is adapted to accommodate the needs of GSM upper layer protocols. Layer 2 supports transmission of frames between MS 40 and BSS 30 or 32. GSM-CDMA Layer 2 includes functionality, such as message ordering, priority and fragmentation, and suspension and resumption of communications, which is normally supported by the standard GSM Layer 2, but not by CDMA IS-95. GSM-CDMA Layer 2 also supports message sizes up to at least the maximum message size permitted by GSM Layer 2 (251 bytes), which is greater than the maximum IS-95 Layer 2 message payload.

Standard GSM protocols include three Radio Interface sub-layers (RIL3) above the physical and framing layers, Layer 1 and Layer 2: Radio Resource (RR) management, Mobile Management (MM) and Connection Management (CM). The CM sub-layer supports signaling for call processing, as well as GSM supplementary services and short message service (SMS). The MM sub-layer supports signaling required for locating MS 40, authentication and encryption key management, as described hereinbelow.

In order to support the substantially unmodified GSM MM and CM sub-layers, a GSM-CDMA RR layer is introduced in the MS 40 and BSS 32 protocol stacks. The GSM-CDMA RR layer, which manages radio resources and maintains radio links between MS 40 and BSSs 30 and 32, is "aware" of the existence of the dual GSM and CDMA lower layers (Layers 1 and 2) in the MS 40 protocol stack. It invokes the appropriate lower layers in the MS stack to communicate with either the standard RIL3-RR layer over the GSM Um interface or the GSM-CDMA RR layer of BSS 32 over the CDMA Um interface, depending on instructions it receives from the BSS with which it is in communication. The RR layer in the MS stack also controls the handover between the corresponding air interfaces defined in Layers 1 and 2, under instructions from MSC 24, BSS 30 and BSS 32.

Regardless of which of the air interfaces is in use, the GSM-CDMA RR layer supports the standard GSM RIL3-MM and CM layers above it. The MM and CM layers are not processed by BSS 32, but are rather relayed through between MS 40 and MSC 24 for processing in a manner substantially transparent to the CDMA air interface layers below. Further features of the RR layer are described in the above-mentioned U.S. patent application serial no. 09/119,717 entitled "Base Station Handover in a Hybrid GSM/CDMA Network."

CDMA BSS 32 communicates with GSM MSC 24 over a standard, substantially unmodified GSM A-interface. This interface is based on the SS7 and BSS Application Part (BSSAP) protocols, as are known in the art, preferably in accordance with the GSM 08.06 and 08.08 standards. BSSAP supports procedures between MSC 24 and BSS 32 that require interpretation and processing of information related to single calls and resource management, as well as transfer of call control and mobility management messages between MSC 24 and MS 40. BSS 32 translates CDMA Layer 1, GSM-CDMA Layer 2 and GSM-CDMA RR protocols exchanged between the BSS and MS 40 into appropriate SS7 and BSSAP protocols for transmission to MSC 24, and vice versa.

Because CDMA BSC 34 communicates with GSM MSC 24 using the standard A-interface, substantially no modifications are required in the core GSM MSC in order to enable the addition of CDMA BSS 32 to GSM system 20. Furthermore, MSC 24 need not be aware that there is any difference in identity between GSM/TDMA BSS 30 and CDMA BSS 32, since both communicate with the MSC in a substantially identical manner over the A-interface.

Fig. 2B is a block diagram that schematically illustrates protocol stacks involved in conveying voice data between MS 40 and MSC 24 via CDMA BSS 32, in accordance with a preferred embodiment of the present invention. Voice data between MS 40 and BSS 32 are coded and decoded by a vocoder particularly suited for CDMA applications, which may comprise any of the standard IS-95 compatible vocoder protocols known in the art. Encryption of the voice data takes place in CDMA Layer 1, along with encryption of signaling and any other user data transmitted between the MS and the BSS. BSS 32 decrypts and translates CDMA Layer 1 into E1 TDMA signals, and converts the CDMA vocoded data into PCM A-law companded voice data, in accordance with the requirements of the A-interface standard. MSC 24 thus transmits and receives voice data to and from MS 40 via BSS 32 substantially without regard to the fact that the data between the BSS and the MS are CDMA-encoded, as though MS 40 were operating in GSM/TDMA mode.

Fig. 3 is a schematic diagram showing message flow between MS 40 (MM and RR protocol layers and SIM 44, as described hereinabove), BSS 32 and MSC 24 associated with encryption of a call, in accordance with a preferred embodiment of the present invention. The call starts with a channel request conveyed by the RR layer of MS 40. BSS 32 responds by allocating a traffic channel to the MS and conveying a long code mask to be used for the call. A link is then opened to MSC 24.

MSC 24 sends an Authentication Request via BSS 32 to MS 40, including a pseudorandom number (RAND), which is input to SIM 44 and used as an indicator in generating a GSM encryption key K_C. Preferably, in accordance with GSM standard 03.20, the SIM inputs the pseudorandom number, together with a key K_i stored in the SIM, to the GSM A8 algorithm to generate K_C, which is conveyed to the MS RR layer for subsequent use in ciphering. SIM 44 returns an Authentication Response to MSC 24, including an indication of K_i, thus enabling the MSC to determine the same key K_c as in MS 40 without transmitting the key over the air.

MSC 24 conveys a GSM Cipher Mode Command message to BSS 32, in accordance with GSM standard 08.08, which is incorporated herein by reference, instructing the BSS to begin encryption. The message contains the GSM encryption key K_C and indicates a ciphering algorithm to be used, typically one of the A5 algorithms, in accordance with GSM standards.

Upon receiving the command, the BSS sends a Ciphering Mode Command to MS 40, substantially in a form specified by GSM standard 04.08, which is incorporated herein by reference. This command contains the indication of the ciphering algorithm received from MSC 24 and any required algorithm-specific information, preferably along with an Action Time, i.e., the CDMA system time at which to start encryption. Since communications between BSS 32 and MS 40 are conducted over the CDMA air interface, however, the BSS and MS preferably do not use GSM ciphering algorithms, but rather use the GSM algorithm indication to select an encryption algorithm compatible with the CDMA air interface. Such algorithms may include suitable stream ciphers and/or spreading using private long codes, as described further hereinbelow.

The RR layer of MS 40 receives and acknowledges the command from the BSS by sending a Ciphering Mode Complete message, preferably within a time equal to T56m (0.2 sec, as specified by the IS-95B standard). GSM-CDMA Layer 2 of MS 40 generates a corresponding acknowledgment message. Alternatively, the MS sends a Ciphering Mode Reject message if it cannot support the required encryption.

At the appropriate Action Time, both BSS 32 and MS 40 switch to the specified encrypted communications mode. The BSS sends a Cipher Mode Complete message to MSC 24, acknowledging successful encryption, and including an International Mobile Equipment Identity (IMEI), as specified by GSM standards, if the IMEI is received from the MS. If the ciphering operation failed, the BSS sends a Cipher Mode Failure Message to the MSC. The RR layer of MS 40 informs the MM layer that the encryption has started, using the RrSyncInd primitive, as specified in GSM standard 04.07, which is incorporated herein by reference.

Any suitable encryption algorithm known in the art may be used to encrypt and decrypt data and signaling between BSS 32 and MS 40. Preferably, the algorithm is of a type that generates a stream cipher, which is obtained by combining the data to be encrypted with a stream of pseudorandom numbers. In the present case, the stream of pseudorandom numbers is generated using the GSM key K_C. Decryption is performed at the

BSS by generating the same pseudorandom number stream and removing it from the encrypted data. The GSM A5/1 ciphering algorithm, for example, works on this principle, but typically requires special-purpose hardware in MS 40 to encrypt and decrypt.

Therefore, the stream ciphering encryption algorithm is most preferably of a type that requires only limited computational power to generate the stream cipher, as described, for example, in U.S. patent application serial nos. 08/934,582 and 08/957,571 both entitled "Method and Apparatus for Generating Encryption Stream Ciphers," respectively filed September 22, 1997 and October 24, 1997, which are assigned to the assignee of the present patent application and both incorporated herein by reference. An exemplary cipher of this type is the SOBER cipher, which can be generated by suitable software running on a general-purpose processor of a type that is commonly used in cellular telephones. The SOBER cipher, based on linear feedback shift registers over a Galois Finite Field of order 2^n, wherein n is chosen for convenience of software implementation, is further described in an article by Greg Rose, entitled "A Stream Cipher Based on Linear Feedback over GF(2^8)," published in the proceedings of the Third Australian Conference on Information Security and Privacy, Springer Verlag (1998), and incorporated herein by reference.

Fig. 4 is a schematic block diagram showing elements of MS 40, including particularly the location therein of encryption operations, in accordance with a preferred embodiment of the present invention. User data, typically comprising voice signals, and signaling are input from TE 46 to a multiplexer 50 in ME 42. An encryption block 52 reads the appropriate GSM encryption key K_c from SIM 44 and ciphers the multiplexed data and signaling using the key, preferably as described hereinabove, in accordance with ciphering instructions from BSS 32. Block 52 may be implemented in hardware and/or software. The encrypted data and signals are then passed through a conventional framing and encoding sequence, as defined by the IS-95 standard and well-known in the art, including a CRC block 54; a frame quality erasure indicator and 8-bit encoder tail block 56; a convolutional encoder 58; a symbol repetition block 60; and an interleaver 62. The interleaved data are input to a 64ary orthogonal modulator 64. A long code generator 70 generates a long code PN spreading sequence code which is shifted as output thereof in accordance with a long code mask received from BSS 32. The code output from long code generator 70 spreads the spectrum of the data, generally in accordance with the IS-95 CDMA standard, using a data burst randomizer 68. The data are finally input to an output stage 72, from which they are transmitted to BSS 32.

Fig. 5 is a schematic block diagram of BSS 32, illustrating elements of the BSS involved in decryption of the data received from MS 40, in accordance with a preferred embodiment of the present invention. The data are received through an input stage 80 of BTS 36. The long code PN spreading is removed using a long code generator 81, similar to long code generator 70 in MS 40. The data are then demodulated, deinterleaved and decoded respectively by a demodulator 83, a deinterleaver 82 and a convolutional decoder 84, and are backhauled to BSC 34. The decoded data are passed through a frame selection block 90 to a decryption block 92, which deciphers the data using the encryption key K_C provided by MSC 24 and an algorithm which is the inverse of whatever ciphering algorithm was used in encryption block 52. The deciphered data are demultiplexed by a demultiplexer 94 to separate out the signaling and voice/data channels that were originally input to ME 42. The separate channels are then suitably routed through GSM/CDMA system 20.

Although MS 40 and BSS 32 have been described hereinabove with reference to encryption and transmission of data by the MS and its reception and decryption by the BSS, it will be understood that the inverse process can similarly be performed to transmit encrypted data from the BSS to the MS.

Fig. 6 is a block diagram illustrating a data structure of a private long code mask 100, generated and used for encryption of transmissions between MS 40 and BSS 32 in accordance with another preferred embodiment of the present invention. As described above with reference to Fig. 4, long code mask 100 is used by the long code generator, which spreads the data before transmission, to provide a shift in the generated code as output from the long code generator. An example of a masked PN code generator is disclosed in U.S. patent no. 5,228,054 issued July 13, 1993 to the assignee of the present application and is incorporated by reference herein. It should be noted that the present invention is described with respect to a long code generator which produces a long code common to all MS. The use of a mask applied to the long code provides a shift in phase of the long code to produce a long code unique to the MS. It should be understood that the mask may also be used in the sense that the long code generator is responsive thereto for producing a long code sequence that does not have any common properties to the long code of any other MS.

In CDMA systems known in the art, the electronic serial number (ESN), from which the public long code mask is derived, is transmitted from the MS to the BSS over an access channel, and is therefore relatively hard for an eavesdropper to intercept. In hybrid GSM/CDMA system 20, however, information pertaining to the long code mask is preferably transmitted from the BSS to the MS over a paging channel (since GSM standards do not recognize the ESN, used in generating the long code mask in accordance with the IS-95 CDMA standard), making it relatively easy for an eavesdropper to capture and decode the call.

For this reason, in the present preferred embodiment, the long code mask is changed after MS 40 has been authenticated to private mask 100. The private long code mask is generated by the MS using GSM encryption key K_C and is not transmitted openly from BSS 32 to MS 40. The key is output by SIM 44 responsive to the pseudorandom indicator number conveyed by MSC 24, as described hereinabove. Beginning at the specified Action Time, as shown in Fig. 3, the private long code mask is by the long code generator in spreading the CDMA data in place of the public long code mask conveyed at the earlier stage of channel assignment. Encryption by long code masking with private mask 100 is preferably used when additional encryption (typically based on SOBER or a GSM ciphering algorithm, as described hereinabove) is not used in encryption block 52.

Long code mask 100 comprises 42 bits, in accordance with the IS-95 standard. Preferably, the two MSB 102 are set to a constant value, and the next six bits 104 are assigned a value by BSS 32 which is varied so that no two

MSs communicating with the BSS have the same long code, even if they by chance have the same K_C. The last thirty-four bits 106 are based on a suitable hash function of K_C. Mask 100, therefore, cannot readily be discovered by an eavesdropper. Bits 104 assigned by BSS 32 ensure that no two calls will have the same long code mask, hence different shifts in the spreading code, since otherwise both calls would be dropped. The use of long code mask 100 thus affords security against call interception and general compatibility with GSM encryption standards with only minimal additional software required in MS 40.

In the course of a call placed through PLMN 22, MS 40 may move from a cell served by one CDMA BSS 32 to another, or between cells served respectively by CDMA BSS 32 and GSM BSS 30. Preferably, when the MS is handed over between the base stations, the ciphering algorithm is switched from the CDMA-compatible algorithms described above to an appropriate GSM algorithm, or vice versa, and ciphering continues substantially uninterrupted.

Although preferred embodiments are described hereinabove with reference to a particular hybrid GSM/CDMA system, it will be appreciated that the principles of the present invention may similarly be applied to provide encryption in other hybrid communication systems, as well. Moreover, although the preferred embodiments make reference to specific TDMA- and CDMA-based communications standards, those skilled in the art will appreciate that the methods and principles described hereinabove may also be used in conjunction with other methods of data encoding and signal modulation. The scope of the present invention encompasses not only the complete systems and communications processes described hereinabove, but also various innovative elements of these systems and processes, as well as combinations and sub-combinations thereof.

It will thus be appreciated that the preferred embodiments described above are cited by way of example, and the full scope of the invention is limited only by the claims.

WE CLAIM:

CLAIMS

1. In a GSM mobile wireless telecommunications system, a method for encrypting data for transmission over a CDMA air interface, comprising:

providing an encryption key in accordance with GSM ciphering protocols; and

encrypting the data for transmission over the CDMA air interface using the key.

2. A method according to claim 1, wherein providing the encryption key comprises exchanging messages indicative of the key over the CDMA air interface substantially in accordance with GSM ciphering protocols.

3. A method according to claim 1, wherein encrypting the data comprises encrypting user data and signaling.

4. A method according to claim 1, wherein encrypting the data comprises generating a stream cipher.

5. A method according to claim 4, wherein generating the stream cipher comprises generating a cipher using a general-purpose microprocessor.

6. A method according to claim 1, wherein encrypting the data comprises generating a masked long code based on the encryption key and applying the masked long code to the data.

7. A method according to claim 6, wherein generating the masked long code comprises generating a mask which includes a group of bits based upon a hash function of the encryption key.

8. A method according to claim 6, wherein generating the masked long code mask comprises generating a mask which includes a group of bits that is different for calls conducted over the CDMA air interface having the same encryption key.

9. A method according to claim 1, wherein encrypting the data comprises:

generating a long code;
generating a long code mask based on the encryption key;
applying the long code mask to the long code; and
applying the masked long code to the data.

10. A method according to claim 9, wherein generating the long code mask comprises generating a group of bits based upon a hash function of the encryption key.

11. A method according to claim 9, wherein generating the long code mask comprises generating a group of bits that is different for calls conducted over the CDMA air interface having the same encryption key.

12. A method according to claim 1, wherein encrypting the data comprises continuing to encrypt data substantially without interruption during a handover between two base stations in the system.

13. A method according to claim 1, wherein encrypting the data comprises encrypting using information stored in a subscriber identity module of a mobile station.

14. Wireless communications apparatus, for use in a GSM mobile telecommunications system, comprising:

a base station, which receives a GSM encryption key from the system and transmits a message indicative of the key over a CDMA air interface; and

a mobile station, which receives the message and responsive thereto derives the key to be used for encrypting data for transmission over the CDMA air interface.

15. Apparatus according to claim 14, wherein the data encrypted by the mobile station include user data and signaling.

16. Apparatus according to claim 14, wherein the base station receives the key and transmits the indication in accordance with GSM messaging protocols.

17. Apparatus according to claim 14, wherein the mobile station comprises a general-purpose microprocessor, which encrypts the data.

18. Apparatus according to claim 14, wherein the mobile station comprises a subscriber identity module and encrypts the data using information received by the mobile station from the module.

19. Apparatus according to claim 14, wherein the mobile station comprises a long code generator, which generates a masked long code in response to the key.

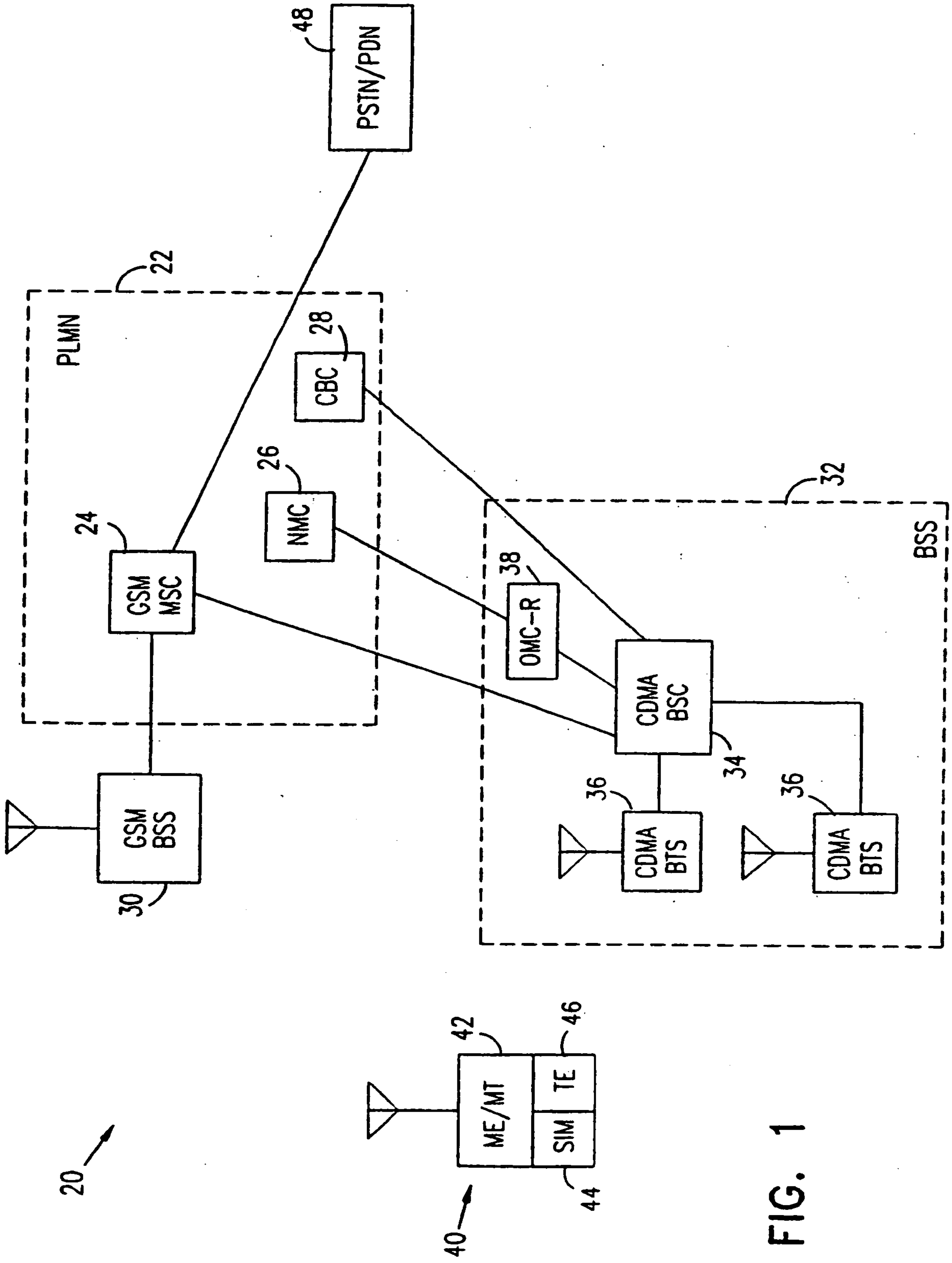

48
PSTN/PDN
22
PLMN
28
CBC
26
NMC
24
GSM MSC
32
BSS
38
OMC-R
CDMA BSC
34
36
CDMA BTS
36
CDMA BTS
GSM BSS
30
42
46
ME/MT
TE
SIM
44
40
20

FIG. 1

FIG. 2A

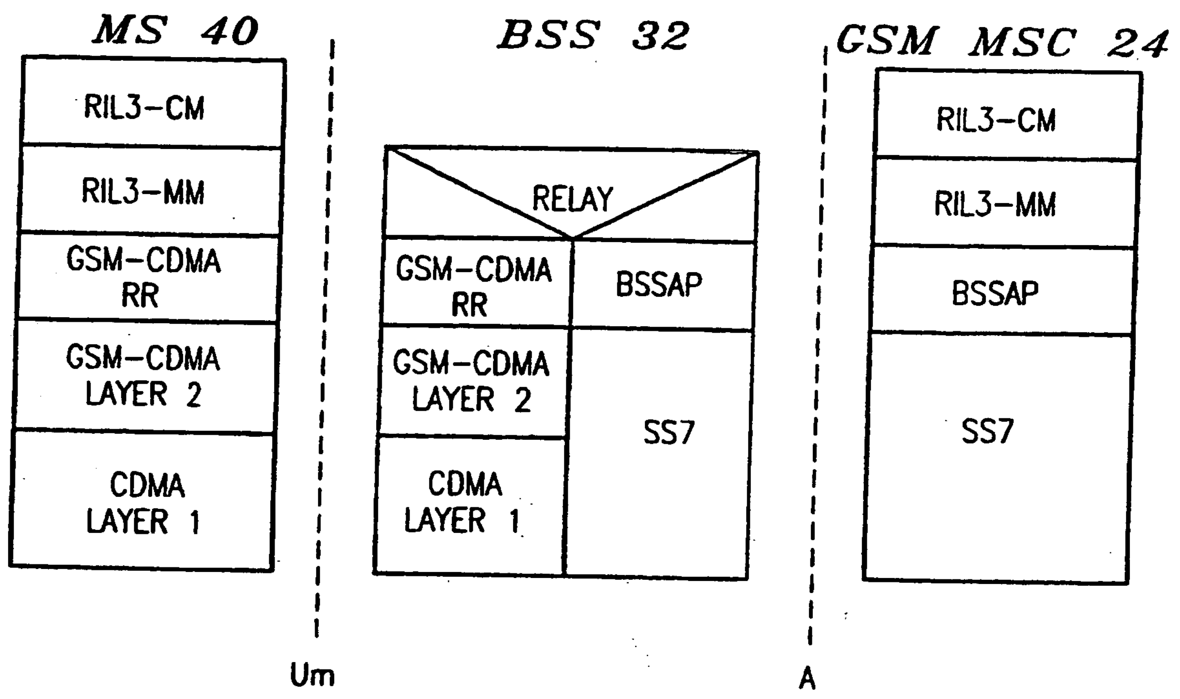
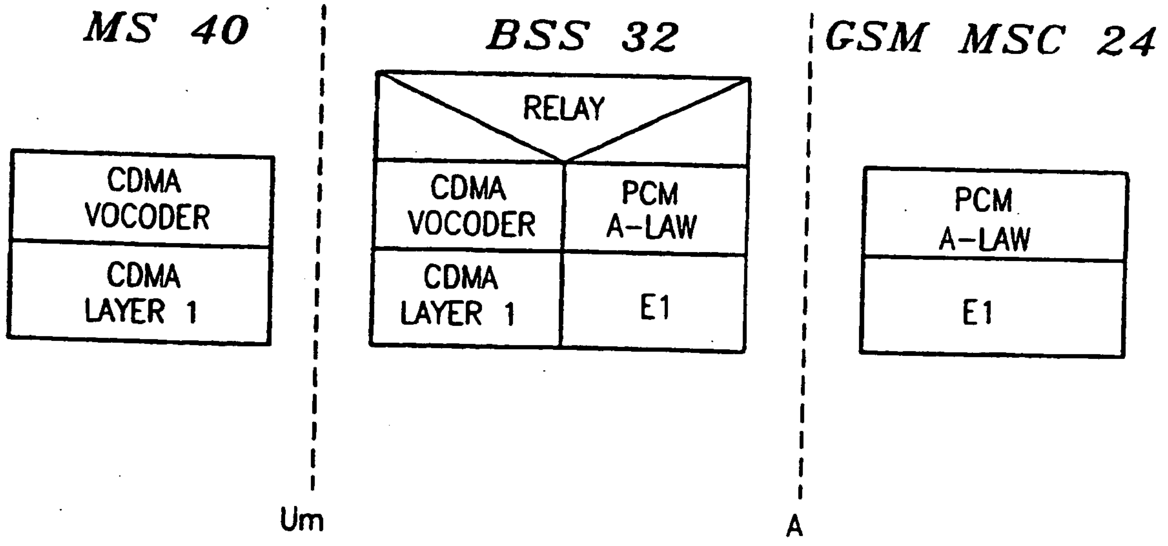

MS 40
RIL3-CM
RIL3-MM
GSM-CDMA RR
GSM-CDMA LAYER 2
CDMA LAYER 1
BSS 32
RELAY
GSM-CDMA RR
BSSAP
GSM-CDMA LAYER 2
SS7
CDMA LAYER 1
GSM MSC 24
RIL3-CM
RIL3-MM
BSSAP
SS7
Um
A

FIG. 2B


MS 40
CDMA VOCODER
CDMA LAYER 1
BSS 32
RELAY
CDMA VOCODER
PCM A-LAW
CDMA LAYER 1
E1
GSM MSC 24
PCM A-LAW
E1
Um
A

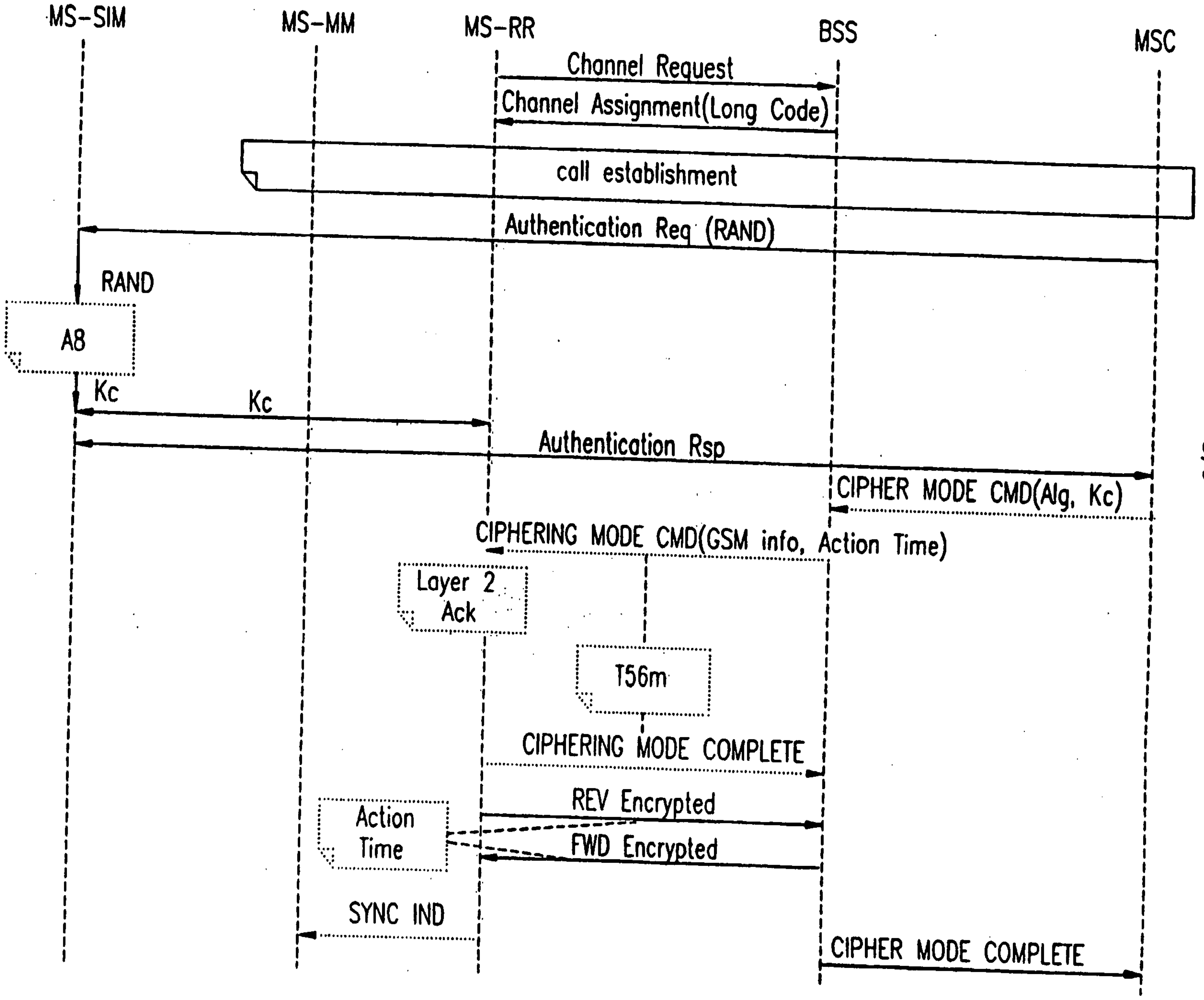
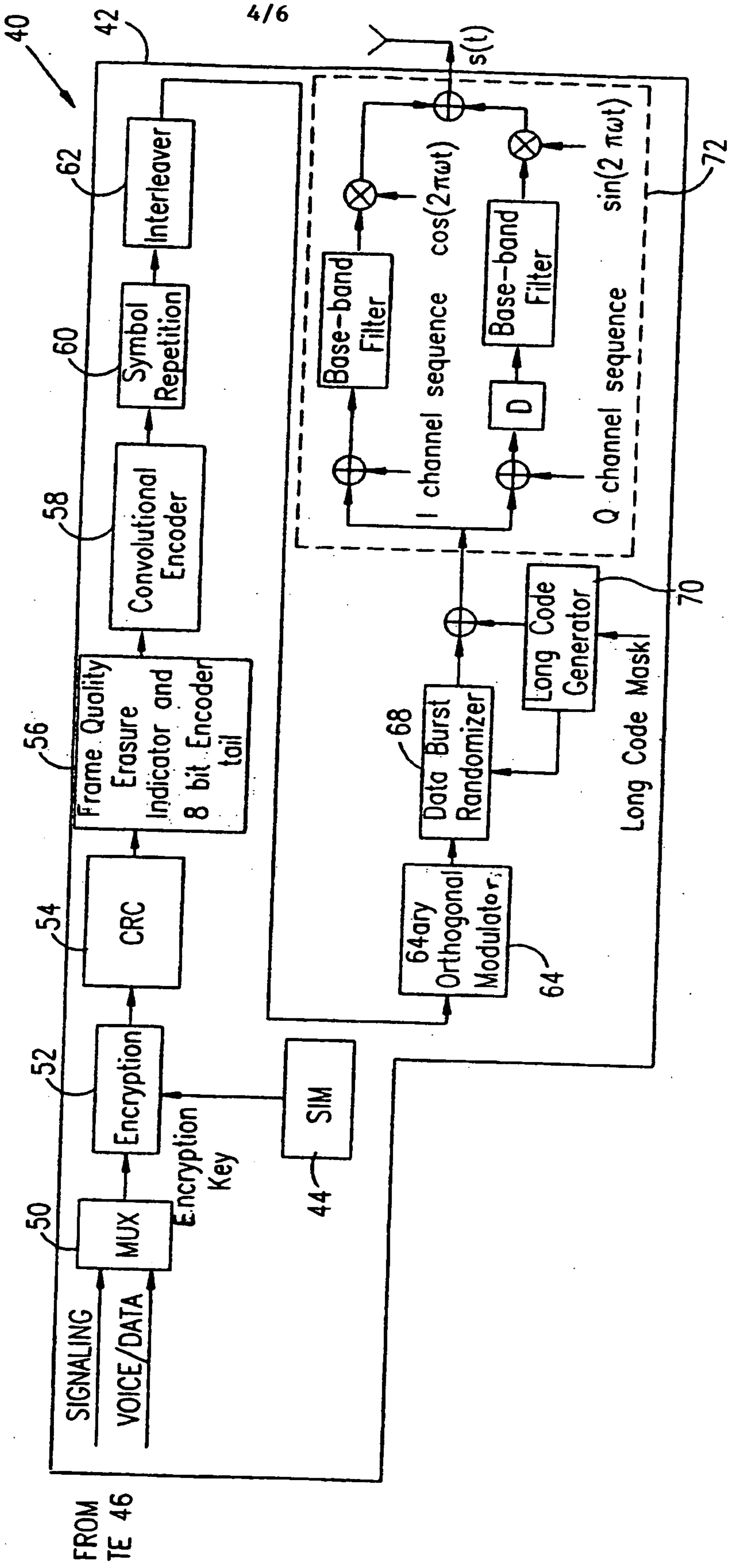

MS-SIM
MS-MM
MS-RR
BSS
MSC
Channel Request
Channel Assignment(Long Code)
call establishment
Authentication Req (RAND)
RAND
A8
Kc
Kc
Authentication Rsp
CIPHER MODE CMD(Alg, Kc)
CIPHERING MODE CMD(GSM info, Action Time)
Layer 2 Ack
T56m
CIPHERING MODE COMPLETE
REV Encrypted
Action Time
FWD Encrypted
SYNC IND
CIPHER MODE COMPLETE

FIG. 3

FIG. 4


40
42
SIGNALING
VOICE/DATA
FROM TE 46
50
MUX
52
Encryption
Encryption Key
SIM
44
54
CRC
56
Frame Quality Erasure Indicator and 8 bit Encoder tail
58
Convolutional Encoder
60
Symbol Repetition
62
Interleaver
64ary Orthogonal Modulator
64
68
Data Burst Randomizer
Long Code Generator
70
Long Code Mask
I channel sequence
Q channel sequence
Base-band Filter
Base-band Filter
D
cos(2πωt)
sin(2 πωt)
s(t)
72

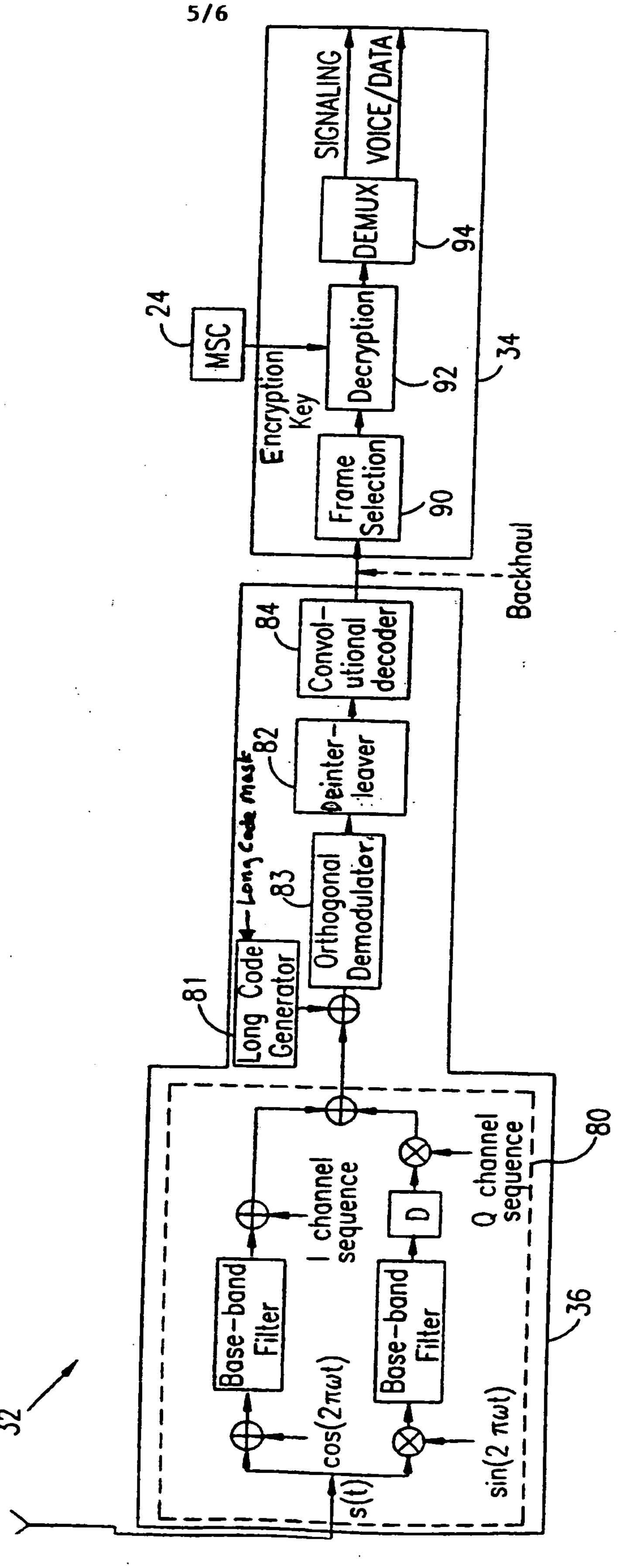

SIGNALING
VOICE/DATA
DEMUX
94
24
MSC
Decryption
92
34
Encryption Key
Frame Selection
90
Backhaul
84
Convol-utional decoder
82
Deinter-leaver
Long Code Mask
83
Orthogonal Demodulator
81
Long Code Generator
80
I channel sequence
Q channel sequence
D
Base-band Filter
Base-band Filter
36
cos(2πωt)
sin(2 πωt)
s(t)
32

FIG. 5

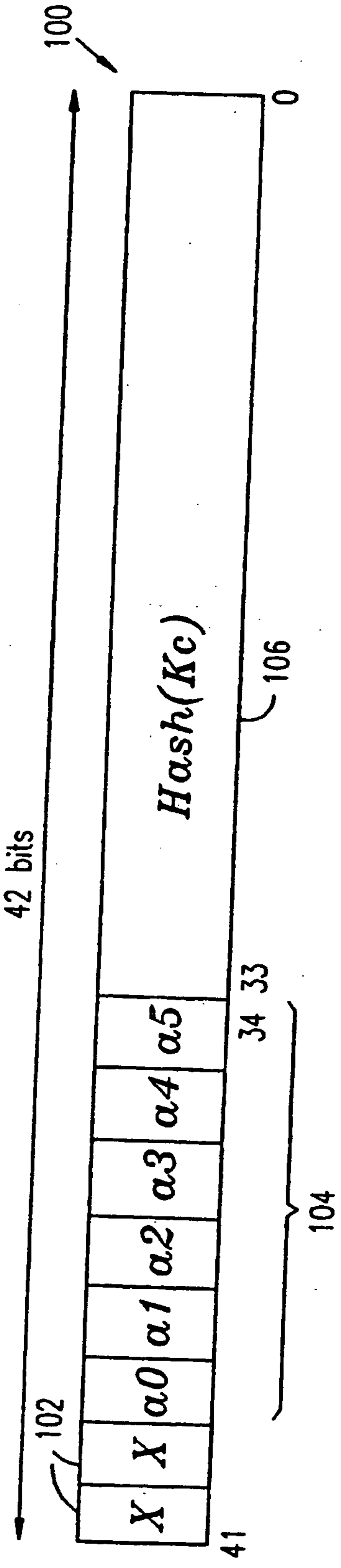


FIG. 6

INTERNATIONAL SEARCH REPORT

Inte onal Application No
PCT/US 99/24521

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 H04B7/216 H04L9/00 H04Q7/22

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 H04B H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	TSCHA Y ET AL: "A subscriber signalling gateway between CDMA mobile station and GSM mobile switching center" 2ND INTERNATIONAL CONFERENCE ON UNIVERSAL PERSONAL COMMUNICATIONS. PERSONAL COMMUNICATIONS: GATEWAY TO THE 21ST CENTURY. CONFERENCE RECORD (CAT. NO.93TH0573-6), PROCEEDINGS OF 2ND IEEE INTERNATIONAL CONFERENCE ON UNIVERSAL PERSONAL COMMUNICATIONS, OT, pages 181-185 vol. 1, XP002128433 1993, New York, NY, USA, IEEE, USA ISBN: 0-7803-1396-8 cited in the application page 183 -page 184 --- -/--	1-19

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 21 January 2000	Date of mailing of the international search report 03/02/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Zucka, G

1

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/US 99/24521

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	COOKE J C ET AL: "Cryptographic security techniques for digital mobile telephones" 1992 IEEE INTERNATIONAL CONFERENCE ON SELECTED TOPICS IN WIRELESS COMMUNICATIONS. CONFERENCE PROCEEDINGS (CAT. NO.92TH0462-2), VANCOUVER, BC, CANADA, 25-26 JUNE 1992, pages 425-428, XP002128434 1992, New York, NY, USA, IEEE, USA ISBN: 0-7803-0723-2 page 425, column 1	1-19
X	WO 97 23108 A (QUALCOMM INC) 26 June 1997 (1997-06-26) cited in the application page 8, line 27 -page 40, line 3	1-19
A	COOKE J C ET AL: "Cryptographic security techniques for digital mobile telephones" SECOND INTERNATIONAL CONFERENCE ON PRIVATE SWITCHING SYSTEMS AND NETWORKS (CONF. PUBL. NO.357), LONDON, UK, 23-25 JUNE 1992, pages 123-130, XP002128435 1992, London, UK, IEE, UK ISBN: 0-85296-546-X page 124, column 2 -page 125	1-19
A	MOELKER D -J ET AL: "Capacity of co-existent cellular CDMA and GSM with shadowing and imperfect sectorization, power control and notch filtering" WAVES OF THE YEAR 2000+ PIMRC '97. THE 8TH IEEE INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE RADIO COMMUNICATIONS. TECHNICAL PROGRAM, PROCEEDINGS (CAT. NO.97TH8271), PROCEEDINGS OF 8TH INTERNATIONAL SYMPOSIUM ON PERSONAL, INDOOR AND MOBILE , pages 27-31 vol.1, XP002128436 1997, New York, NY, USA, IEEE, USA ISBN: 0-7803-3871-5	1,14
A	WO 96 21999 A (NOKIA TELECOMMUNICATIONS OY ;LAATU JUHO (FI); MAEENPAEAE SANNA (FI) 18 July 1996 (1996-07-18) cited in the application page 2, line 6 -page 12, line 35	1,14
A	US 5 228 054 A (RUETH TIMOTHY I ET AL) 13 July 1993 (1993-07-13) cited in the application column 3, line 6 -column 10, line 54	1,14

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ional Application No
PCT/US 99/24521

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9723108 A	26-06-1997	US 5878036 A	02-03-1999
		AU 1689397 A	14-07-1997
		CA 2241007 A	26-06-1997
		CN 1186586 A	01-07-1998
		EP 0811298 A	10-12-1997
		FI 972991 A	22-09-1997
		HU 9900984 A	28-07-1999
WO 9621999 A	18-07-1996	US 5664004 A	02-09-1997
		AU 700659 B	14-01-1999
		AU 4439996 A	31-07-1996
		CA 2210006 A	18-07-1996
		CN 1173961 A	18-02-1998
		EP 0803167 A	29-10-1997
		FI 972973 A	11-07-1997
		JP 10512121 T	17-11-1998
		NO 973233 A	11-09-1997
US 5228054 A	13-07-1993	AU 4045593 A	08-11-1993
		CN 1082284 A	16-02-1994
		IL 105207 A	16-10-1996
		MX 9301917 A	31-08-1994
		WO 9320630 A	14-10-1993
		ZA 9302097 A	12-01-1994